Functional Hazard Assessments

Brett Portwood

Technical Specialist, Safety and Integration

(562) 627-5350

brett.portwood@faa.gov

FHA PROCESS

- Start With List of System/Aircraft Functions
- Postulate Hazards Based on the Failures in These Functions
- Derive Overall Effect of Hazard on System/Aircraft and People - Failure Condition
- Assess Severity of Failure Condition - Assign Classification

FHA

- Provides the Top Level Design Criteria
- Determines the Depth of Further Analyses
- Allows for Derivation of the System Architecture
- Independent of Hardware

FHA

- When To Do Or Revise It
  - Early in the design process
  - Revise when functions are added, deleted, altered, or used in different applications
  - As a final check, it is prudent to review the FHA again at the end of the program.

Function Description

- Should describe the aircraft or system function to the degree necessary to analyze the function with respect to loss of function and malfunction (misuse and external events/environmental effects may also need to be considered)

PHASES OF FLIGHT EXAMPLES

- Ground
  - Maintenance
  - Engine Start
  - Taxi
  - Shutdown
- Take-off
  - Before take-off
  - < V1, < Vr, etc.
  - Rejected
- In Flight
  - Climb Obstacle
  - Climb Cruise
  - Cruise
  - Descent
  - Approach
  - 500ft to touchdown

Aircraft Failure Condition Examples

- Loss of flightpath control
  - Loss of pitch axis control
  - Loss of roll axis control
  - Loss of yaw axis control
  - Loss of multi axis control
- Flightpath control malfunction
  - Pitch axis hardover
  - Pitch axis slowover
  - Pitch axis ocsillations
  - Roll …..
  - Yaw …..
  - Multi axis …..

System Failure Condition Examples

- Autopilot
  - Annunciated Roll Hardover /Slowover
  - Unannunciated Pitch Hardover/ slowover
- Autothrottle
  - Unable to hold speed target
  - Throttle hardovers/ slowovers
- Loss of all displayed airspeed
- Un-annuciated misleading airspeed on one display

Hazard Description Examples Effect on Aircraft and Crew

- Loss of Flight Director
  - All phases
    - Increased crew workload in take-off, approach, and go-around modes (assumes aircraft can be flown using raw data)
- Misleading Flight Director Commands
  - Take-off and approach phases
    - Pilot may not fly proper reference at low altitude. Could possibly fly into terrain.

Hazard Severity

- The effects of failures or development errors of a function on the aircraft, crew, or occupants.
  - Based mainly on historical service history of a particular aircraft type (e.g. small transport, large transport, helicopter, small general aviation, etc.)
  - Severity should be established by experienced safety engineers with input from an experienced cross-section of specialists.

Why Aircraft Level FHA ??

- Historically, aircraft systems were relatively separate entities that operated independently of each other
  - Steam Gauge Instruments
  - Little or no integration
  - No software

Why Aircraft Level FTA ??

- Advent of computer-based digital systems
  - Tremendous increase in integration
  - Flexibility in adding/changing functionality
  - Complex Software
  - Complex Hardware
  - Commercial Off-the Shelf (COTs) hardware/software
  - Generic Computing Resources

Aircraft Level FHA

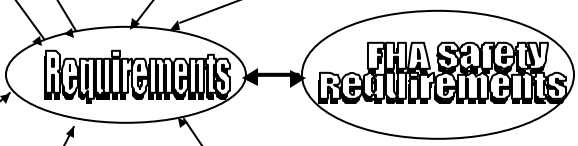
- Complex systems that are integrated and perform multiple aircraft level functions can cause non-intuitive hazards.
  - A structured top down analysis method is necessary to address potential safety concerns.

Why Aircraft Level FHA ??

- Systems that use similar architectures and complex components in performing multiple aircraft functions can introduce additional aircraft failure conditions involving multiple functions
- Therefore, it is beneficial to assess functions at the highest appropriate level

Requirements Capture

- Customer
- Operational
- Interface
- Performance
- Physical/Installation
- Maintainability
- Certification Requirements

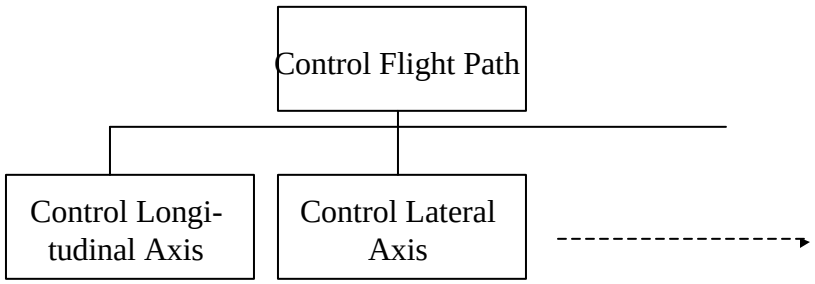


AIRCRAFT LEVEL FUNCTIONS

- How many aircraft level functions define an aircraft ?
  - Depends on how aircraft functions are defined
  - Should be defined at the “highest appropriate” level.
    - Depends on overall knowledge and experience
    - Requires consultation with experienced specialists
    - Failure Condition definitions/classifications can change based on system allocation decisions.

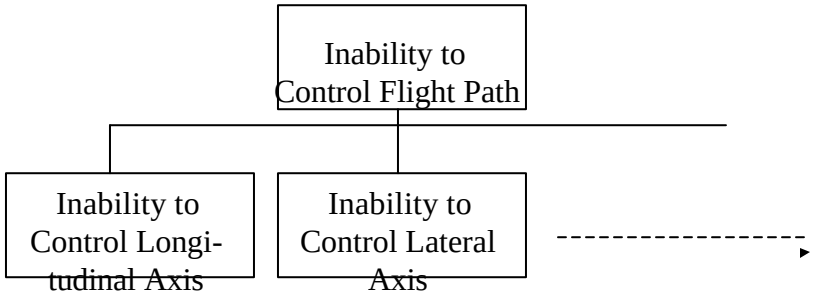
Aircraft Level FHA

- Function Trees
  - Can help "visualize" functional hierarchy



Aircraft Level FHA

- Functional Failure Conditions



Aircraft Level FHA

- Inability to Control Lateral Axis
  - Loss of Lateral Control
  - Erroneous Lateral Control Inability to Control
- Longitudinal Axis
  - Loss of Longitudinal Control
  - Erroneous Longitudinal Control
    - Longitudinal Slowover
    - Longitudinal Hardover
    - Oscillatory Malfunction

Aircraft Level FHA

- Eventually, the aircraft level failure conditions should be defined together with their respective safety objectives along with the proposed means for demonstrating compliance.
- Establishing a general hazard list for future projects is a good idea

Aircraft Level FHA

- Interative Nature
  - For highly integrated systems which perform multiple aircraft level functions then the initial Aircraft Level FHA may need to be revised during the system allocation process to identify and classify the new failure conditions involving multiple functions, or..
  - If systems use similar architecture or identical complex components the new failure conditions should be accounted for.

Aircraft Level FHA

- The overall objective is to account for failure conditions that occur across multiple systems that may effect multiple aircraft level functions.
- A system level FHA often does not address this aspect of a System Safety Assessment.

Aircraft Level FHA

- Implementation choices made during development may introduce common causes for multiple aircraft failure conditions or interactions between systems resulting in cross-system or cross-functional failures.
  - Reviews as part of the common cause analysis should be performed to determine if such conditions exist and if they should be added to Aircraft Level FHA

Aircraft Level FHA

- CAUTION
  - For extremely integrated architectures that involve multiple aircraft level functions, an Aircraft Level FHA may require several iterations as lower (system) level design decisions are made to properly identify the effects of common software and/or common complex hardware on aircraft level failure conditions.

Caution

- Exercise care when aircraft level functions are not independent.
- Must convey in FHA
  - Use of remarks/comments appropriate
  - May need to redefine/clarify failure conditions

Frequently Asked Question

- If there are mitigating factors (e.g. crew annunciation, back-up systems, monitors, etc.) to lower the failure condition classification level, say for example, from catastrophic to hazardous, do I include the lower level in the FHA or do I include the non-mitigated failure condition classification level in the FHA ??

Answer

- Both ways are acceptable IF:
  - Enough information is included to clearly identify each failure condition along with THE RATIONALE for its severity classification.
    - Some applicants use a two column format
      - One column is the severity without mitigation
      - A second column is the mitigated severity

Example

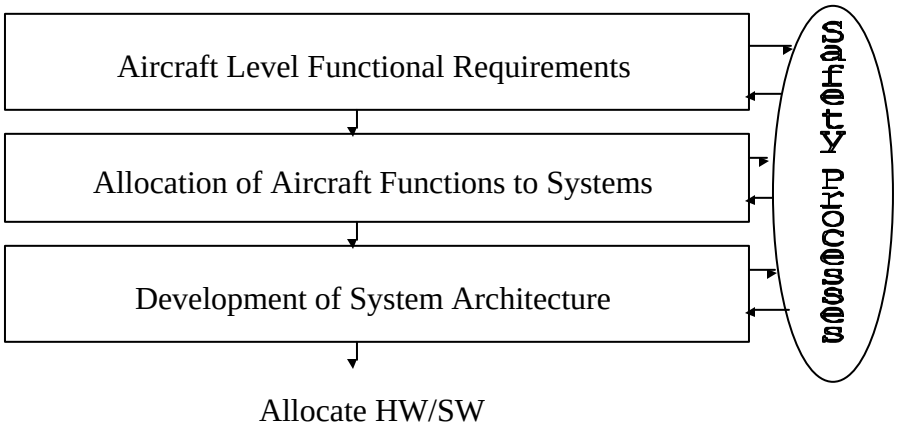
Failure Condition	Classification	Classification without proper crew action (Un-mitigated)
Annunciated loss of deceleration capability on the ground	Major (Divert to long runway with overrun area)	Catastrophic (Crew does not interpret annuciated information)

Example

- The information on the FHA for this failure condition tells us:
  - Information to help assess minimum DAL of deceleration system components and annunciation system components.
  - Information to assist in validating the crew alerting system (with pilot/human factors input)

System Level Functional Hazard Assessments

Allocation of Aircraft Functions to Systems



System Level FHA

- Same basic process as Aircraft level FHA except:
  - Failure Conditions are described at the system level as opposed to the aircraft level.
  - It considers a failure or combination failures at the *SYSTEM* level that affect an aircraft level function.

System Level FHA

- Like the Aircraft Level FHA, the System Level FHA is also iterative in nature.
  - Each system that integrates multiple aircraft functions should be re-examined using the System Level FHA process.
  - If separate systems or sub-systems use similar architectures or identical complex components and introduce additional system level failure conditions, the the System FHA should be modified to include them.

EXAMPLE SYSTEM FHA MATRIX

Function	Hazard	Phase	Failure Condition	Class.	Certification Approach	Remarks
Stick-Shaker	Loss	Flight-w/ speed margin	None	Minor	Flight Test	
		Flight-near Stall	Increases prob. of aircraft entering Stall	Major	FMEA	1. Dual stick-shaker channels 2. A/C provides natural buffet 3. Low speed protection autothrottle
	False Warning	<V1	Possible rejected Take-off	Major	FMEA	1. Inhibit shaker V1 until 200 ft.

Traceability Between Aircraft Level and System Level

- Traceability of hazards and failure conditions between the system level and aircraft level is necessary.
  - Provides a means to determine compatibility of System reliability budgets and Sub-system reliability budgets
  - Provides a means to validate the proposed Design Assurance Levels (DALs)

QUESTIONS OR COMMENTS